

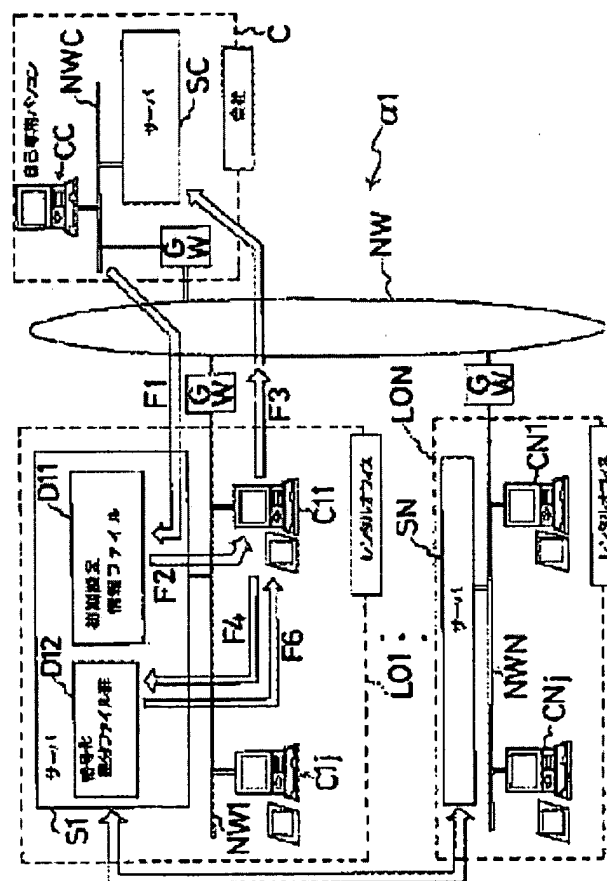
USING METHOD AND SYSTEM DEVICE FOR SHARED COMPUTER

Patent number: JP2002140295
Publication date: 2002-05-17
Inventor: NAKAHAMA KIYOSHI
Applicant: NIPPON TELEGRAPH & TELEPHONE
Classification:
 - international: G06F15/00; G06F9/445; G06F13/00
 - european:
Application number: JP20000335566 20001102
Priority number(s): JP20000335566 20001102

Report a data error here

Abstract of JP2002140295

PROBLEM TO BE SOLVED: To provide a shared computer using method and a system device capable of constructing an environment of a personal computer used once in a personal computer in another location at once, minimizing the traffic, and minimizing the server load and file capacity in each location.
SOLUTION: In this adopted characteristic construction method, the backup of a use environment is carried out in a server S1 when a shared computer C11 governed by the server S1 (first server) in one location (rental office LO1) is used, and encryption differential information stored in the server S1 (first server) is copied in a server SN (second server) only when a synergistic computer CN1 governed by the server SN (second server) in another location (rental office LON) is used after the shared computer C11 is used.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-140295

(P 2002-140295 A)

(43) 公開日 平成14年5月17日 (2002.5.17)

| (51) Int. Cl. ⁷ | 識別記号 | F I | テーマコード (参考) | | |
|----------------------------|------|------------|-------------|---|-------|
| G06F 15/00 | 310 | G06F 15/00 | 310 | U | 5B076 |
| 9/445 | | 13/00 | 500 | A | 5B085 |
| 13/00 | 500 | 9/06 | 610 | A | |

審査請求 未請求 請求項の数15 O L (全16頁)

(21) 出願番号 特願2000-335566 (P 2000-335566)

(22) 出願日 平成12年11月2日 (2000.11.2)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 中濱 清志

東京都千代田区大手町二丁目3番1号 日

本電信電話株式会社内

(74) 代理人 100071113

弁理士 菅 隆彦

Fターム (参考) 5B076 AA02

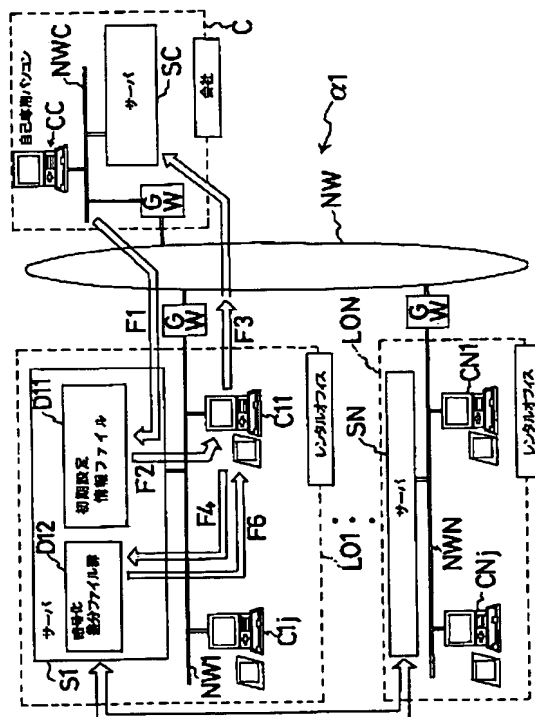
5B085 BG04

(54) 【発明の名称】 共同利用コンピュータ利用方法及びシステム装置

(57) 【要約】

【課題】 一度使用したパソコンの環境を別の拠点のパソコンでも即座に構築可能とし、トラフィックを最小限にし、各拠点のサーバの負荷及びファイル容量を最小限にすることが可能な共同利用コンピュータ利用方法及びシステム装置の提供。

【解決手段】 ある拠点（レンタルオフィスLO1）のサーバS1（第1サーバ）支配下の共同利用コンピュータC11が利用されたときに、サーバS1に利用環境のバックアップを行ない、共同利用コンピュータC11の利用後に、他の拠点（レンタルオフィスLON）のサーバSN（第2サーバ）支配下の共同利用コンピュータCN1を使用する場合にのみ、サーバS1（第1サーバ）に記憶された暗号化差分情報を、サーバSN（第2サーバ）に複写する特徴的構成手法の採用。



【特許請求の範囲】

【請求項 1】現に使用する特定の共同利用コンピュータにおいて設定・記憶させる情報を当該特定の共同利用コンピュータにおいて暗号化し、当該暗号化した暗号文を当該特定の共同利用コンピュータに対するサーバの記憶手段に暗号化差分情報として記憶させておく利用環境のバックアップを行ない、

当該サーバに接続可能な共同利用コンピュータを別途使用する際に当該暗号化差分情報を当該共同利用コンピュータにて復号化して使用する利用環境の復元を行なう共同利用コンピュータ利用方法であって、

前記サーバが複数の拠点それぞれに配置されており、前記利用環境のバックアップをする前記サーバの一つである第 1 サーバと、当該第 1 サーバが配置されている拠点とは異なる拠点に配置されていて前記利用環境の復元をする前記サーバの一つである第 2 サーバと、を用い、前記第 1 サーバの支配下の共同利用コンピュータが利用されたときに、当該第 1 サーバに当該利用環境のバックアップを行ない、当該第 1 サーバの支配下の共同利用コンピュータの利用後に、前記第 2 サーバの支配下の共同利用コンピュータを使用する場合にのみ、当該第 1 サーバに記憶された前記暗号化差分情報を、当該第 2 サーバに複写する、

ことを特徴とする共同利用コンピュータ利用方法。

【請求項 2】前記第 1 サーバと前記第 2 サーバとは、通信網を介して通信を行ない、当該第 1 サーバから当該第 2 サーバへの前記暗号化差分情報の複写は、当該通信網を介して行なう、ことを特徴とする請求項 1 に記載の共同利用コンピュータ利用方法。

【請求項 3】前記第 1 サーバに記憶された前記暗号化差分情報の前記第 2 サーバへの複写は、当該第 1 サーバの支配下の共同利用コンピュータの利用後であって、当該第 2 サーバの支配下の共同利用コンピュータを使用する前に、当該第 2 サーバにつき WEB ブラウザを用いて指定する手法を用いる、ことを特徴とする請求項 1 又は 2 に記載の共同利用コンピュータ利用方法。

【請求項 4】前記第 2 サーバは、当該第 2 サーバの支配下の共同利用コンピュータが利用されるときに、前記第 1 サーバより複写した前記暗号化差分情報に基づいて、当該第 1 サーバの利用環境を復元することにより、

前記第 1 サーバの支配下の共同利用コンピュータと前記第 2 サーバの支配下の共同利用コンピュータとで、同一の利用環境を復元する、

ことを特徴とする請求項 1 又は 2 に記載の共同利用コンピュータ利用方法。

【請求項 5】前記暗号化と前記復号化は、共同利用コンピュータの利用者のみが利用できる IC カ

ードに記憶させた鍵を用いて行ない、

共同利用コンピュータの利用後に、当該共同利用コンピュータの記憶手段に記憶させた情報の全てを削除しておき、

その後、共同利用コンピュータを利用する際に、前記第 2 サーバに複写された前記暗号化差分情報を前記鍵により復号して再度利用する、

ことを特徴とする請求項 1、2、3 又は 4 に記載の共同利用コンピュータ利用方法。

【請求項 6】前記再度利用は、

ユーザ認証をして正当性が確認された利用者のみが当該再度利用することが可能となり、

現に再度利用する特定の共同利用コンピュータが前記第 2 サーバから前記暗号化差分情報を取得し、当該取得した暗号文を前記 IC カードに記憶させた鍵により復号化して、当該特定の共同利用コンピュータの記憶手段に記憶させて、前記使用した環境を当該再度利用する特定の共同利用コンピュータに構築する、

ことを特徴とする請求項 5 に記載の共同利用コンピュータ利用方法。

【請求項 7】前記利用環境のバックアップは、

利用者固有の利用環境からなる初期設定情報を初期設定情報ファイルとして前記サーバ上に作成する処理と、当該初期設定情報ファイルを他の全ての前記サーバに複写する処理と、を実施する、

ことを特徴とする請求項 1、2、3、4、5 又は 6 に記載の共同利用コンピュータ利用方法。

【請求項 8】前記暗号化差分情報は、

前記利用者が前記特定の共同利用コンピュータに設定するメール設定情報、アクセス環境情報、ブラウザ設定情報の何れかを含む通信環境情報、辞書設定情報の 1 以上を含んでなる環境情報と、

前記利用者がインターネットを含む外部通信網を介し前記特定の共同利用コンピュータを用いて作成したファイル群の暗号文と、を有する、

ことを特徴とする請求項 1、2、3、4、5、6 又は 7 に記載の共同利用コンピュータ利用方法。

【請求項 9】現に使用する特定の共同利用コンピュータにおいて設定・記憶させる情報を当該特定の共同利用コンピュータにおいて暗号化し、当該暗号化した暗号文を当該特定の共同利用コンピュータに対するサーバの記憶手段に暗号化差分情報として記憶させておく利用環境のバックアップを行ない、

当該サーバに接続可能な共同利用コンピュータを別途使用する際に当該暗号化差分情報を当該共同利用コンピュータにて復号化して使用する利用環境の復元を行なう共同利用コンピュータ利用方法であって、

前記サーバが複数の拠点それぞれに配置されており、前記利用環境のバックアップをする前記サーバの一つである第 1 サーバと、当該第 1 サーバが配置されている拠点

10

20

30

40

50

とは異なる拠点に配置されていて前記利用環境の復元をする前記サーバの一つである第2サーバと、を用い、前記第1サーバと前記第2サーバとは、通信網を介して通信を行ない、当該第1サーバから当該第2サーバへの前記暗号化差分情報の複写は、当該通信網を介して行ない、

前記第1サーバの支配下の共同利用コンピュータが利用されたときに、当該第1サーバに当該利用環境のバックアップを行ない、当該第1サーバの支配下の共同利用コンピュータの利用後に、前記第2サーバの支配下の共同利用コンピュータを使用する場合にのみ、当該第2サーバの支配下の共同利用コンピュータを使用する前に、当該第2サーバにつきWEBブラウザを用いて指定すること、

当該第1サーバに記憶された前記暗号化差分情報を、当該第2サーバに前記通信網経由で複写し、

その後、前記第2サーバが、当該第2サーバの支配下の共同利用コンピュータが利用されるときに、前記第1サーバより複写した前記暗号化差分情報に基づいて、当該第1サーバの利用環境を当該第2サーバの支配下の共同利用コンピュータに復元することにより、

前記第1サーバの支配下の共同利用コンピュータと前記第2サーバの支配下の共同利用コンピュータとで、同一の利用環境を復元する、

ことを特徴とする共同利用コンピュータ利用方法。

【請求項10】複数の拠点それぞれに配置されているサーバと、複数の拠点それぞれに配置されていて当該拠点の前記サーバに内部通信網で接続されていて複数の利用者に利用される共同利用コンピュータと、を有し、各拠点の内部通信網同士が外部通信網を介して接続されてなる共同利用コンピュータシステム装置であって、前記共同利用コンピュータは、

当該共同利用コンピュータにおいて設定・記憶させる情報を暗号化し、当該暗号化した暗号文を当該共同利用コンピュータと同一拠点内の前記サーバに暗号化差分情報として記憶させる暗号化サーバ読み書き手段と、前記サーバに記憶されている前記暗号化差分情報を復号化して利用環境の復元をする復号化サーバ読み書き手段と、を有し、

前記サーバは、

前記サーバの一つである第1サーバの支配下の共同利用コンピュータが利用され、その後当該第1サーバとは異なる拠点に配置された前記サーバの一つである第2サーバが利用される場合にのみ、当該第1サーバに記憶された前記暗号化差分情報を、当該第2サーバに前記外部通信網経由で複写する複写手段を有する、

ことを特徴とする共同利用コンピュータシステム装置。

【請求項11】前記複写手段は、

前記第1サーバと前記第2サーバとの間で相互にアクセス可能とするWEBブラウザを有する、

ことを特徴とする請求項10に記載の共同利用コンピュータシステム装置。

【請求項12】前記複写手段は、

利用者の正当性を認証する認証手段を有する、

ことを特徴とする請求項10又は11に記載の共同利用コンピュータシステム装置。

【請求項13】前記共同利用コンピュータの復号化サーバ読み書き手段は、

前記第1サーバより前記第2サーバに複写された前記暗号化差分情報に基づいて、当該第1サーバ支配下の共同利用コンピュータの利用環境を、当該第2サーバ支配下の共同利用コンピュータに復元するものからなる、

ことを特徴とする請求項10、11又は12に記載の共同利用コンピュータシステム装置。

【請求項14】前記共同利用コンピュータシステム装置は、

前記暗号化及び復号化をするときに用いられる鍵を記憶するICカードを使用要件とする、

ことを特徴とする請求項10、11、12又は13に記載の共同利用コンピュータシステム装置。

【請求項15】前記共同利用コンピュータは、

利用者固有の利用環境からなる初期設定情報を初期設定情報ファイルとして、各拠点のすべての前記サーバ上に作成するメイン制御手段を、有する、

ことを特徴とする請求項10、11、12、13又は14に記載の共同利用コンピュータシステム装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、レンタルオフィス、リモートオフィスといった共同利用形態であっても汎用オペレーションシステムのコンピュータ（パソコン）をハイセキュリティに使用可能にする共同利用コンピュータ利用方法及びその実施に直接使用するシステム装置に関するものである。

【0002】

【従来の技術】従来、レンタルオフィス、リモートオフィスでは、その場所に存在する汎用オペレーションシステムのパソコンを共同で利用するか（かかるパソコンを共同利用パソコンとする）、又は、各自でパソコンを持ち込んで利用する（かかるパソコンを持込パソコンとする）必要があった。

【0003】

【発明が解決しようとする課題】しかしながら、持込パソコンを使用する場合には、ネットワークの設定といった個別の設定事項は、自分専用にすることができ、使用環境のカスタマイズは実現できるものの、パソコン自体を持ち運ぶことが必須条件となり不便であった。

【0004】一方、共同利用パソコン（一般のスタンドアローンパソコン、OSはWindows95、同98、MACOSなど）を使用する場合、自分の会社のネットワークにリモ

ート接続したり、また、インターネットに接続したりする為に、利用する前に、事前に、ネットワークの接続を変更したり、メールソフトの各種の設定を行うことを余儀なくされ、日本語の入力に際しても、日本語の辞書なども共同利用となる為、効率が悪く不便であり、ファイルをハードディスクに保存する際のセキュリティについて、常に利用者自身が注意を払う必要があった。

【0005】このようなセキュリティについての問題点を解決する方法としては、特願平11-206026号に記載されているところの共同利用コンピュータ利用方法が考え出されている。この共同利用コンピュータ利用方法では、第1の効果として、利用者がパソコンを利用する際に、自分が以前使用していた環境を引き続き別のパソコンで使用することが可能となり、第2の効果として、共同利用パソコンが複数箇所に設置されている場合であって、その設置箇所がそれぞれ別の場所である場合でも第1の効果を達成できる。

【0006】即ち、特願平11-206026号に記載されている共同利用コンピュータ利用方法では、使用環境をバックアップしたパソコンと、その使用環境を復元するパソコンが別であり、それぞれ別の場所に設置されている場合でも、従前の使用環境を不都合なく復元することを可能とする。

【0007】上述の第1の効果を実現する手段としては、共同利用コンピュータにおいて、利用者が使った情報を当該共同利用コンピュータにおいて暗号化し、暗号化した暗号文を当該共同利用コンピュータに対するサーバの記憶手段に暗号化差分情報として記憶させておき（以下、利用環境のバックアップとする）、当該サーバに接続可能な共同利用コンピュータを別途使用する際に当該暗号化差分情報を当該共同利用コンピュータにて復号する（以下、利用環境の復元とする）手法が、特願平11-206026号に記載されている。

【0008】上述の第2の効果を実現する手段としては、複数存在する拠点のすべてに設けられていてそれぞれ外部通信網に接続されたサーバに、それぞれ暗号化差分情報を保存させ、当該暗号化差分情報を外部通信網経由ですべて自動更新（以下、暗号化差分情報のミラーリングとする）で同期させることにより、第1のサーバで利用環境のバックアップを行ない、当該利用環境につき第2のサーバで復元する共同利用コンピュータの利用手法が、特願平11-206026号の「発明の実施の形態」などに記載されている。

【0009】しかしながら、特願平11-206026号の上述の第2の効果を実現する手法では、不要なトラフィックが生じる場合がある。例えば、ある利用者が同一のサーバの支配下にある共同利用コンピュータのみを利用する場合は、暗号差分情報のミラーリングを行なうことはまったく意味をなさない。また、この場合は、不要なトラフィックが発生するだけでなく、ミラーリン

グのためのサーバの無用な負荷及び無用なディスク領域確保の必要性も発生する。

【0010】ここにおいて、本発明の解決すべき主要な目的は以下の通りである。即ち、本発明の第1の目的は、複数の拠点それぞれで共同利用コンピュータを利用する場合に、トラフィックを最小限にすることを可能とする共同利用コンピュータ利用方法及びシステム装置を提供せんとするものである。

【0011】本発明の第2の目的は、複数の拠点それぞれで共同利用コンピュータを利用する場合に、各拠点それぞれに配置されたサーバの負荷を最小限にすることを可能とする共同利用コンピュータ利用方法及びシステム装置を提供せんとするものである。

【0012】本発明の第3の目的は、複数の拠点それぞれで共同利用コンピュータを利用する場合に、各拠点それぞれに配置されたサーバのファイル容量を最小限にすることを可能とする共同利用コンピュータ利用方法及びシステム装置を提供せんとするものである。

【0013】本発明の第4の目的は、利用した共同利用コンピュータでの環境を別の拠点の共同利用コンピュータにおいても即座に構築可能とするものであって、トラフィックを最小限にし、各拠点のサーバの負荷及びファイル容量を最小限にすることを可能とする共同利用コンピュータ利用方法及びシステム装置を提供せんとするものである。

【0014】本発明の第5の目的は、利用者が構築した環境及び利用者の作成したファイルに関して当該利用者が注意を払うことを前提とせず高いセキュリティを維持することが可能であって、利用した共同利用コンピュータでの環境を別の拠点の共同利用コンピュータにおいても即座に構築可能で、且つトラフィックを最小限にし、各拠点のサーバの負荷及びファイル容量を最小限にすることを可能とする共同利用コンピュータ利用方法及びシステム装置を提供せんとするものである。

【0015】本発明の他の目的は、明細書、図面、特に、特許請求の範囲における各請求項の記載から自ずと明らかとなろう。

【0016】

【課題を解決するための手段】本発明方法は、上記課題の解決に当たり、サーバが複数の拠点それぞれに配置されており、利用環境のバックアップをする前記サーバの一つである第1サーバと、当該第1サーバが配置されている拠点とは異なる拠点に配置されていて前記利用環境の復元をする前記サーバの一つである第2サーバと、を用い、前記第1サーバの支配下の共同利用コンピュータが利用されたときに、当該第1サーバに当該利用環境のバックアップを行ない、当該第1サーバの支配下の共同利用コンピュータの利用後に、前記第2サーバの支配下の共同利用コンピュータを使用する場合にのみ、当該第1サーバに記憶された前記暗号化差分情報を、当該第2

サーバに複写してなる構成手法を講じる特徴を有する。

【0017】本発明システム装置は、上記課題の解決に当たり、各拠点に配置されている共同利用コンピュータは、当該共同利用コンピュータの利用環境を暗号化し、当該暗号化した利用環境をサーバに暗号化差分情報として記憶させる暗号化サーバ読み書き手段と、前記サーバに記憶されている前記暗号化差分情報を復号化して利用環境の復元をする復号化サーバ読み書き手段と、を有し、各拠点に配置されている前記サーバは、当該サーバの一つである第1サーバの支配下の共同利用コンピュータが利用され、その後当該第1サーバとは異なる拠点に配置された前記サーバの一つである第2サーバが利用される場合にのみ、当該第1サーバに記憶された前記暗号化差分情報を、当該第2サーバに外部通信網経由で複写する複写手段を有してなる構成手法を講じる特徴を有する。

【0018】更に、具体的詳細に述べると、当該課題の解決では、本発明が次に列挙する上位概念から下位概念にわたる新規な特徴的構成手法又は手段を採用することにより、上記目的を達成するように為される。

【0019】即ち、本発明方法の第1の特徴は、現に使用する特定の共同利用コンピュータにおいて設定・記憶させる情報を当該特定の共同利用コンピュータにおいて暗号化し、当該暗号化した暗号文を当該特定の共同利用コンピュータに対するサーバの記憶手段に暗号化差分情報として記憶させておく利用環境のバックアップを行ない、当該サーバに接続可能な共同利用コンピュータを別途使用する際に当該暗号化差分情報を当該共同利用コンピュータにて復号化して使用する利用環境の復元を行なう共同利用コンピュータ利用方法であって、前記サーバが複数の拠点それぞれに配置されており、前記利用環境のバックアップをする前記サーバの一つである第1サーバと、当該第1サーバが配置されている拠点とは異なる拠点に配置されていて前記利用環境の復元をする前記サーバの一つである第2サーバと、を用い、前記第1サーバの支配下の共同利用コンピュータが利用されたときに、当該第1サーバに当該利用環境のバックアップを行ない、当該第1サーバの支配下の共同利用コンピュータの利用後に、前記第2サーバの支配下の共同利用コンピュータを使用する場合にのみ、当該第1サーバに記憶された前記暗号化差分情報を、当該第2サーバに複写してなる共同利用コンピュータ利用方法の構成採用にある。

【0020】本発明方法の第2の特徴は、上記本発明方法の第1の特徴における前記第1サーバと前記第2サーバとが、通信網を介して通信を行ない、当該第1サーバから当該第2サーバへの前記暗号化差分情報の複写は、当該通信網を介して実施してなる共同利用コンピュータ利用方法の構成採用にある。

【0021】本発明方法の第3の特徴は、上記本発明方法の第1又は第2の特徴における前記第1サーバに記憶

された前記暗号化差分情報の前記第2サーバへの複写が、当該第1サーバの支配下の共同利用コンピュータの利用後であって、当該第2サーバの支配下の共同利用コンピュータを使用する前に、当該第2サーバにつきWEBブラウザを用いて指定する手法を用いてなる共同利用コンピュータ利用方法の構成採用にある。

【0022】本発明方法の第4の特徴は、上記本発明方法の第1又は第2の特徴における前記第2サーバが、当該第2サーバの支配下の共同利用コンピュータが利用されるときに、前記第1サーバより複写した前記暗号化差分情報に基づいて、当該第1サーバの利用環境を復元することにより、前記第1サーバの支配下の共同利用コンピュータと前記第2サーバの支配下の共同利用コンピュータとで、同一の利用環境を復元してなる共同利用コンピュータ利用方法の構成採用にある。

【0023】本発明方法の第5の特徴は、上記本発明方法の第1、第2、第3又は第4の特徴における前記暗号化と前記復号化が、共同利用コンピュータの利用者のみを使用できるICカードに記憶させた鍵を用いて行ない、共同利用コンピュータの利用後に、当該共同利用コンピュータの記憶手段に記憶させた情報の全てを削除しておき、その後、共同利用コンピュータを利用する際に、前記第2サーバに複写された前記暗号化差分情報を前記鍵により復号して再度利用してなる共同利用コンピュータ利用方法の構成採用にある。

【0024】本発明方法の第6の特徴は、上記本発明方法の第5の特徴における前記再度利用が、ユーザ認証をして正当性が確認された利用者のみが当該再度利用することが可能となり、現に再度利用する特定の共同利用コンピュータが前記第2サーバから前記暗号化差分情報を取得し、当該取得した暗号文を前記ICカードに記憶させた鍵により復号化して、当該特定の共同利用コンピュータの記憶手段に記憶させて、前記使用した環境を当該再度利用する特定の共同利用コンピュータに構築してなる共同利用コンピュータ利用方法の構成採用にある。

【0025】本発明方法の第7の特徴は、上記本発明方法の第1、第2、第3、第4、第5又は第6の特徴における前記利用環境のバックアップが、利用者固有の利用環境からなる初期設定情報を初期設定情報ファイルとして前記サーバ上に作成する処理と、当該初期設定情報ファイルを他の全ての前記サーバに複写する処理と、を実施してなる共同利用コンピュータ利用方法の構成採用にある。

【0026】本発明方法の第8の特徴は、上記本発明方法の第1、第2、第3、第4、第5、第6又は第7の特徴における前記暗号化差分情報が、前記利用者が前記特定の共同利用コンピュータに設定するメール設定情報、アクセス環境情報、ブラウザ設定情報の何れかを含む通信環境情報、辞書設定情報の1以上を含んでなる環境情報と、前記利用者がインターネットを含む外部通信網を

10

20

30

40

50

介し前記特定の共同利用コンピュータを用いて作成したファイル群の暗号文と、を有してなる共同利用コンピュータ利用方法の構成採用にある。

【0027】本発明方法の第9の特徴は、現に使用する特定の共同利用コンピュータにおいて設定・記憶させる情報を当該特定の共同利用コンピュータにおいて暗号化し、当該暗号化した暗号文を当該特定の共同利用コンピュータに対するサーバの記憶手段に暗号化差分情報として記憶させておく利用環境のバックアップを行ない、当該サーバに接続可能な共同利用コンピュータを別途使用する際に当該暗号化差分情報を当該共同利用コンピュータにて復号化して使用する利用環境の復元を行なう共同利用コンピュータ利用方法であって、前記サーバが複数の拠点それぞれに配置されており、前記利用環境のバックアップをする前記サーバの一つである第1サーバと、当該第1サーバが配置されている拠点とは異なる拠点に配置されていて前記利用環境の復元をする前記サーバの一つである第2サーバと、を用い、前記第1サーバと前記第2サーバとは、通信網を介して通信を行ない、当該第1サーバから当該第2サーバへの前記暗号化差分情報の複写は、当該通信網を介して行ない、前記第1サーバの支配下の共同利用コンピュータが利用されたときに、当該第1サーバに当該利用環境のバックアップを行ない、当該第1サーバの支配下の共同利用コンピュータの利用後に、前記第2サーバの支配下の共同利用コンピュータを使用する場合にのみ、当該第2サーバの支配下の共同利用コンピュータを使用する前に、当該第2サーバにつきWEBブラウザを用いて指定することで、当該第1サーバに記憶された前記暗号化差分情報を、当該第2サーバに前記通信網経由で複写し、その後、前記第2サーバが、当該第2サーバの支配下の共同利用コンピュータが利用されるときに、前記第1サーバより複写した前記暗号化差分情報に基づいて、当該第1サーバの利用環境を当該第2サーバの支配下の共同利用コンピュータに復元することにより、前記第1サーバの支配下の共同利用コンピュータと前記第2サーバの支配下の共同利用コンピュータとで、同一の利用環境を復元してなる共同利用コンピュータ利用方法の構成採用にある。

【0028】本発明システム装置の第1の特徴は、複数の拠点それぞれに配置されているサーバと、複数の拠点それぞれに配置されていて当該拠点の前記サーバに内部通信網で接続されていて複数の利用者に利用される共同利用コンピュータと、を有し、各拠点の内部通信網同士が外部通信網を介して接続されてなる共同利用コンピュータシステム装置であって、前記共同利用コンピュータは、当該共同利用コンピュータにおいて設定・記憶させる情報を暗号化し、当該暗号化した暗号文を当該共同利用コンピュータと同一拠点内の前記サーバに暗号化差分情報として記憶させる暗号化サーバ読み書き手段と、前記サーバに記憶されている前記暗号化差分情報を復号化

して利用環境の復元をする復号化サーバ読み書き手段と、を有し、前記サーバは、前記サーバの一つである第1サーバの支配下の共同利用コンピュータが利用され、その後に当該第1サーバとは異なる拠点に配置された前記サーバの一つである第2サーバが利用される場合のみ、当該第1サーバに記憶された前記暗号化差分情報を、当該第2サーバに前記外部通信網経由で複写する複写手段を有するものからなる共同利用コンピュータシステム装置の構成採用にある。

【0029】本発明システム装置の第2の特徴は、上記本発明システム装置の第1の特徴における前記複写手段が、前記第1サーバと前記第2サーバとの間で相互にアクセス可能とするWEBブラウザを有してなる共同利用コンピュータシステム装置の構成採用にある。

【0030】本発明システム装置の第3の特徴は、上記本発明システム装置の第1又は第2の特徴における前記複写手段が、利用者の正当性を認証する認証手段を有してなる共同利用コンピュータシステム装置の構成採用にある。

【0031】本発明システム装置の第4の特徴は、上記本発明システム装置の第1、第2又は第3の特徴における前記共同利用コンピュータの復号化サーバ読み書き手段が、前記第1サーバより前記第2サーバに複写された前記暗号化差分情報に基づいて、当該第1サーバ支配下の共同利用コンピュータの利用環境を、当該第2サーバ支配下の共同利用コンピュータに復元するものからなる共同利用コンピュータシステム装置の構成採用にある。

【0032】本発明システム装置の第5の特徴は、上記本発明システム装置の第1、第2、第3又は第4の特徴における前記共同利用コンピュータシステム装置が、前記暗号化及び復号化をするときに用いられる鍵を記憶するICカードを使用要件としてなる共同利用コンピュータシステム装置の構成採用にある。

【0033】本発明システム装置の第6の特徴は、上記本発明システム装置の第1、第2、第3、第4又は第5の特徴における前記共同利用コンピュータが、利用者固有の利用環境からなる初期設定情報を初期設定情報ファイルとして、各拠点のすべての前記サーバ上に作成するメイン制御手段を、有してなる共同利用コンピュータシステム装置の構成採用にある。

【0034】

【発明の実施の形態】以下、添付図面を参照しながら、本発明の実施の形態を共同利用コンピュータシステム装置及び共同利用コンピュータ利用方法につき説明する。

【0035】本発明の実施形態を説明する前に、本発明を実現可能にする共同利用コンピュータシステム装置、特にシェアードピシィ (Shared PC、SPC)、について説明をする。当該シェアードピシィは、外出中のビジネスマン等が自分のオフィスと同様のパソコン環境で仕事を行うことを可能にするパソコンで

あり、共同作業スペース（レンタルオフィス、自分の会社内の共同作業スペース等）に設置される。

【0036】ここで、ターゲットとなる利用者は、例えば、外出中に、会社・学校・インターネットのメールを読んだり、インターネット接続でネットサーフィンを行いたいビジネスマン・学生等の者のみならず、出張先などの出先にてオフィス等のパソコンアプリケーションで利用作成を行いたい者、スケジュールの合間などに時間を潰したい者などが挙げられる。

【0037】共同利用パソコン（シェアードピシィ）には、OSとして汎用OS（Windows98、MACOS等）を採用し、標準的なアプリケーション（文書作成ソフト、メールソフト、WEBブラウザ）を何種類かインストール済みとし、ユーザが共同で利用する。

【0038】なお、本発明は複数の拠点（例えばレンタルオフィス）それぞれで共同利用コンピュータを利用する際に用いられるものであるが、本実施形態では共同利用コンピュータの代表例として専ら共同利用パソコン

（パソコン）を挙げて説明しているも、本発明はこれに限定されるものではなく、共同利用コンピュータとして汎用コンピュータ、携帯電話、PHSなどを用いてもよい。

【0039】（共同利用コンピュータシステム装置）以下、添付図面を参照しながら、共同利用コンピュータシステム装置につき説明する。図1は共同利用コンピュータシステム装置 α 、図2は共同利用コンピュータシステム装置 α 1のそれぞれ構成図である。なお、システム装置自体の構成は、図1乃至図2に示す共同利用コンピュータシステム装置 α 、 α 1以外の他の構成であっても良く、当該構成の規模、通信網の整備規模等の状況に応じて、又利用者のニーズに応じて適宜変更し得る。

【0040】図1に示す共同利用コンピュータシステム装置 α につき説明する。共同利用コンピュータシステム装置 α は、会社Cに構築されているLANなどの内部通信網NWCと、レンタルオフィスLO1に構築されているLANなどの内部通信網NW1とを、それぞれゲートウェイGWを介してインターネットを始めとする外部の各種情報通信網NWと接続自在とするシステム装置構成である。

【0041】会社Cに構築されている内部通信網NWCには、サーバSC及びパソコンが接続されている。説明上、パソコンのうち自己専用パソコンCCを一台取り上げて説明する。通常、利用者は、自己専用パソコンCCからサーバSCにアクセスして、メールの読み書き、各種のネットワークサービス、ファイルサーバアクセスといった社内ネットワークサービスを利用しているほか、自己専用パソコンCC内で資料作成などを行っている。

【0042】一方、レンタルオフィスLO1の内部通信網NW1には、利用者用のパソコン（共同利用パソコン、以下単にパソコンとする）C1j（添え字jは、レ

ンタルオフィスLO1にあるパソコンのナンバー1～Mに該当、一台でもよい）が接続されると共に、当該内部通信網NW1上のサーバS1が接続されている。サーバS1には、初期設定情報ファイルD11と暗号化差分ファイル群D12なるデータが、適宜蓄積し得る。何時どのような場合に蓄積されるかについては、詳細を後述する。

【0043】共同利用コンピュータシステム装置 α は、レンタルオフィスLO1に利用者が任意の契機で赴き、会社Cの自分専用のパソコンCCと同一の利用環境にてパソコンC1jを利用可能にするシステム装置である。その為、作業環境を、保存（バックアップ）したり、復元（レストア）する為のサーバS1が必ず必要となる。

【0044】図2に示す共同利用コンピュータシステム装置 α 1は、図1に示した共同利用コンピュータシステム装置 α の別形態であり、レンタルオフィスLO1、LO2、・・・、LONという様に複数のレンタルオフィスが存在する場合である。

【0045】レンタルオフィスLOk（添え字kはレンタルオフィスのナンバーであり、1～Nの任意の数）は、共同利用コンピュータシステム装置 α におけるレンタルオフィスの一つの拠点であり、何れも図1におけるレンタルオフィスLO1と同一の構成であり、サーバSk及びパソコンCk1、・・・、Ckj（添え字kは1～Nの任意の数でLOkのkと対応）が存在する。

【0046】本発明の実施形態は、共同利用コンピュータシステム装置 α 1の構成を用いるものであり、共同利用コンピュータシステム装置 α 1の構成において、何れのパソコンC11、・・・、Cnjからでも作業環境の保存及び復元をすることが出来る方法を提供するものである。

【0047】（共同利用コンピュータ利用方法）本発明の実施形態は、先に述べたとおり図2における共同利用コンピュータシステム装置 α 1の構成を用いた共同利用コンピュータ利用方法である。しかし、本実施形態の特徴を記載する為には、本実施形態のベースとなる共同利用コンピュータシステム装置 α の共同利用コンピュータ利用方法の説明をすることが必要である。共同利用コンピュータシステム装置 α 1については、共同利用コンピュータシステム装置 α の説明の後に、詳細に説明する。

【0048】以下、図1を参照しながら、共同利用コンピュータシステム装置 α においてレンタルオフィスLO1に設置されたパソコンC11の本利用手順を説明することにより、共同利用コンピュータ利用方法を説明する。

【0049】＜初回利用手順＞まず、レンタルオフィスLO1を初めて利用する場合の流れを説明することにする。ここでのポイントは、レンタルオフィスLO1に赴くと、ユーザ毎にカスタマイズされた環境（ネットワーク、環境などの利用環境）から作業を直ちに開始できる

ことにある。

【0050】初めて利用する場合には、以下の(手順1)～(手順5)に従うことになる。手順1は、次の通りである。利用者は、レンタルオフィスL01を使用するに当たり、初回の利用時には、前もって、会社C(自己専用パソコンC1)からサーバS1にアクセスして、社内の内部通信網NWCへのアクセス権や辞書などの環境を、初期設定情報ファイルD11に登録しておく(F1)。

【0051】手順2は、次の通りである。利用者が、レンタルオフィスL01の利用を思い立ち、レンタルオフィスL01に赴くと、例えばパソコンC11を利用できる位置にいることになるが、パソコンC11の利用に先立ち、初回の利用時には、利用者の正当性を認証すると共に、手順1で登録した環境を、初期設定情報ファイルD11を基に当該パソコンC11に構築する(F2)。

【0052】手順3は、次の通りである。上記手順2により環境が構築されたパソコンC11を使用して、会社CのサーバSCの利用、インターネットへの接続、各種文書等の作成を行う(F3)。

【0053】手順4は、次の通りである。パソコンC11の利用が終了の際に、利用環境(パソコンC11に記憶させた情報も含む)をサーバS1の暗号化差分ファイル群D12として保存する。之には、パソコンC11から削除した情報は暗号化差分ファイル群D12から削除されることも含まれる(F4)。なお、手順3において、パソコンC11のハードディスクの変化に応じて、任意に、又は定期的に手順4を行ってもよい。

【0054】手順5は、次の通りである。パソコンC11内の情報を全て完全に消去する。例えば、利用したハードディスクHDをフォーマットする。これにより、セキュリティを保護することができる。

【0055】上記した様に、初回利用の利用者の行動と利用手順は、手順1→手順2→手順3→手順4→手順5を、標準とする。

【0056】＜2回目以降の手順＞次に、2回目以降の利用手順につき説明を行う。2回目以降は、前回の作業環境から、パソコンの利用を継続可能にし、以下の手順で行う。

【0057】手順6は、次の通りである。利用者が、2回目以降にレンタルオフィスL01の使用を思い立ち、レンタルオフィスL01に赴くと、パソコンC11(前回使用したパソコンと同一である必要性はない、図3参照)を利用できる位置にいるが、パソコンC11を使用するに先立ち、2回目以降の利用時に、利用者の正当性を認証し、前回手順4で保存した環境を、暗号化差分ファイル群D12からパソコンC11に復元する(F6)。

【0058】それ以降は、上記手順3、手順4、手順5を順に行う。即ち、2回目以降の利用者の行動及び利用

手順は、手順6→手順3→手順4→手順5を、標準とする。

【0059】次に、図2を参照しながら、本発明の実施形態である共同利用コンピュータシステム装置α1の形態、即ち複数のレンタルオフィスが存在し、各々にサーバが存在する場合の共同利用コンピュータ利用方法について説明する。

【0060】＜初回利用手順＞先ず、レンタルオフィスL01を初めて利用する場合の流れを説明することにする。ここでのポイントは、レンタルオフィスL01に赴くと、ユーザ毎にカスタマイズされた環境(ネットワーク、環境などの利用環境)から作業を直ちに開始できることにある。

【0061】初めて利用する場合には、以下の(手順1)～(手順5)に従うことになる。手順1は、次の通りである。利用者は、レンタルオフィスL01を使用するに当たり、初回の利用時には、前もって、会社C(自己専用パソコンC1)からサーバS1にアクセスして、社内の内部通信網NWCへのアクセス権や辞書などの環境を、初期設定情報ファイルD11に登録しておく(F1)。

【0062】手順1'は、次の通りである。初期設定情報ファイルD11が登録されると、サーバS1～SNに対して、初期設定情報ファイルD11をコピーすることにより、全てのサーバにつき初期設定情報ファイルD11を作成する(F1')。

【0063】手順2は、次の通りである。利用者が、レンタルオフィスL01の利用を思い立ち、レンタルオフィスL01に赴くと、例えばパソコンC11を利用できる位置にいることになるが、パソコンC11の利用に先立ち、初回の利用時には、利用者の正当性を認証すると共に、手順1で登録した環境を、初期設定情報ファイルD11を基に当該パソコンC11に構築する(F2)。

【0064】手順3は、次の通りである。上記手順2により環境が構築されたパソコンC11を使用して、会社CのサーバSCの利用、インターネットへの接続、各種文書等の作成を行う(F3)。

【0065】手順4は、次の通りである。パソコンC11の利用が終了の際に、利用環境(パソコンC11に記憶させた情報も含む)をサーバS1の暗号化差分ファイル群D12として保存する。之には、パソコンC11から削除した情報は暗号化差分ファイル群D12から削除されることも含まれる(F4)。なお、手順3において、パソコンC11のハードディスクの変化に応じて、任意に、又は定期的に手順4を行ってもよい。

【0066】手順5は、次の通りである。パソコンC11内の情報を全て完全に消去する。例えば、利用したハードディスクHDをフォーマットする。これにより、セキュリティを保護することができる。

【0067】上記したように、初回利用の利用者の行動

と利用手順は、手順1→手順1'→手順2→手順3→手順4→手順5を、標準とする。

【0068】<2回目以降の手順>前回利用したレンタルオフィスを、レンタルオフィスLOp（添え字pは前回利用したレンタルオフィスの番号であり、1～Nは任意の数）とする。説明を簡略化するために、前回利用したレンタルオフィスの番号p=1の場合について、以下に説明する。2回目以降に使用を思い立ったレンタルオフィスがレンタルオフィスLO1の場合は、上述の（共同利用コンピュータ利用方法）における<2回目以降の手順>と同様であるので説明を割愛する。

【0069】手順9は、次の通りである。2回目以降に使用を思い立ったレンタルオフィスがレンタルオフィスLOk（k≠1）の場合は、レンタルオフィスLOkに赴く前に、WEBブラウザ等で、前回利用したレンタルオフィスのサーバS1にアクセスし、ユーザ認証後、次に利用するレンタルオフィスがレンタルオフィスLOkであることをWEBブラウザから入力する（F9-1）。それを受けてサーバS1上の暗号化差分ファイル群D12をサーバSkにコピーする（F9-2）。

【0070】手順6は、次の通りである。利用者が、2回目以降にレンタルオフィスLOkの使用を思い立ち、レンタルオフィスLOkに赴くと、パソコンCk1（前回使用したパソコンと同一である必要性はない、図3参照）を利用できる位置にいるが、パソコンCk1を使用するに先立ち、2回目以降の利用時に、利用者の正当性を認証し、前回手順4で保存した環境を、暗号化差分ファイル群D12からパソコンC11に復元する（F6）。

【0071】それ以降は、上記手順3、手順4、手順5を順に行う。即ち、2回目以降の利用者の行動及び利用手順は、手順9→手順6→手順3→手順4→手順5を、標準とする。

【0072】

【実施例】以下、実施例について、共同利用コンピュータシステム装置α1を用いた共同利用コンピュータ利用方法を、詳細に説明する。図4は、共同利用コンピュータシステム装置αの内部構成を示したものである。

【0073】なお、図には、本発明の実施に必要となる範囲の内部構成であり、当然に通常のサーバ、パソコンに備わる機能は含まれており、図面上省略してある。また、図4の内部構成は、図1に示した共同利用コンピュータシステム装置αに限らず、図2、図3に示した共同利用コンピュータシステム装置α1であっても同様であり、図4では、その内部構成及び機能、ひいては本発明の差分情報利用方法を説明するための図面であり、内部通信網NWC、NW1、・・・、外部通信網NW、ゲートウェイGW等はラインLで示してある。また、矢印は各種情報のやり取りを示す。

【0074】共同利用パソコンC1j（jは任意の数）

には、CDROM1を読むCDROMドライブ2、共同利用パソコンC1jを使用する際に必要となるICカード3を読み取るICカードR/W4、キーボード、マウス、マイク等の入力手段5を備え、内部には、当該共同利用パソコンの内部を制御するメイン制御手段6、ICカード3に記憶されている情報への読み書きを行うカード情報読み書き手段7、初期設定情報ファイルD11の情報からスクリプトを作成し当該作成したスクリプトをハードディスクHDに記憶させるスクリプト作成手段8、ハードディスクHDに記憶させたスクリプトを実行するスクリプト実行手段9、CDROM1の情報から共通初期アプリケーション環境をハードディスクHDに構築する共通初期アプリケーション復元手段10、サーバS1の暗号化差分ファイル群D12とハードディスクHDの情報とを比較しコピーファイルリスト及び削除ファイルリストから成る差分リストを抽出する差分抽出手段11、差分抽出手段11から差分リストを基にコピーファイルリストのファイル群を暗号化し暗号化差分ファイル群D12に記憶させ削除ファイルリストのファイル群を暗号化差分ファイル群D12から削除する一方、暗号化差分ファイル群D12の各ファイルを復号しハードディスクHDに記憶させる暗号／復号化サーバ読み書き手段12、ハードディスクHDなどの記録手段で構成される。

【0075】サーバS1は、設定登録手段21、CGIプログラム22、初期設定情報ファイルD11、CDROM作成時刻情報23、暗号化差分ファイル群D12を最低限備える。自己専用パソコンC1には、辞書31、ブックマーク32など利用環境と、WEBブラウザ／FTPクライアント33を備える。

【0076】ここで、図1及び図4を参照しながら、上記手順に従い、共同利用コンピュータシステム装置α各部の詳細を含め共同利用コンピュータ利用方法の実施例につき、説明する。なお、上記手順のうち、手順3及び手順5については、周知事項であるので、説明を省略する。

【0077】なお、共同利用コンピュータシステム装置αを使用するに先立ち、利用者には、利用に必携となる利用者毎にICカード3が交付されており、ICカード3には、当該ICカード3のカードID（カードID=i）、鍵Xi、当該ICカード3に固有のカードパスワードが登録されている。ここでのカードIDのiと鍵Xiの添え字iとは同一の番号である。

【0078】カードIDは利用者を特定するためのIDであり、鍵は暗号化の鍵であり、カードパスワードはICカード3を持っている利用者の正当性をカード内で確認するものであり、カードパスワードを入力手段5にて入力し照合（ICカード3内での照合が望ましい）を経ないと、当該ICカード3にはアクセス不能とする。また、カードID及びカードパスワードの登録時に、鍵X

i は自動生成されることが望ましい。ここで、利用者は、自己のカードパスワード及びカードIDを記憶しているものとするが、鍵Xiについては、ICカード3内生成されるので、利用者が知る必要性はない。

【0079】<<手順1>>手順1は、利用環境を事前に登録する手順である。利用者は会社Cの自己専用パソコンCから、レンタルオフィスLO1のサーバS1上で起動中の設定登録手段21にアクセスして、パソコン環境をサーバS1に登録する。具体的には、以下の通りである。

【0080】先ず、自己専用パソコンCからサーバS1上で起動中の設定登録手段21（WEBサーバでなど構成）にアクセスすると、CGIプログラム22が起動され、設定登録手段21が表示する設定画面が自己専用パソコンCに表示される。当該画面の一例を図5に示す。利用者は、入力手段5を用いて、表示された設定画面WEBブラウザなどから、ユーザ名、カードID、パスワード、メールソフト種別（画面から選択）、POPサーバ名、SMTPサーバ名、メールアカウント、漢字変換IME（画面から選択）、WEBブラウザ種別（画面から選択）、辞書ファイル、WEBブックマークファイルなどの初期設定データを入力する（手順1-1）。

【0081】このとき、メールソフト種別、POPサーバ名、SMTPサーバ名、メールアカウント、漢字変換IME、WEBブラウザ種別、辞書ファイル、WEBのブックマークファイルについては、自己専用パソコンSCと同一の環境を利用する場合には、自己専用パソコンCのハードディスクHD中の情報を自動的にサーチして、設定入力を自動化することもできる。

【0082】そして、CGIプログラム22が、設定登録手段21から初期設定データを受け取り、カードID=iをキーとした初期設定情報ファイルD11を作成する（手順1-2）。

【0083】なお、以降、説明上、メールソフト種別、POPサーバ名、SMTPサーバ名及びメールアカウントをまとめてメール情報、IME種別及び辞書ファイルをまとめて辞書情報、WEBブラウザ種別及びブックマークをまとめてブラウザ情報と呼び、更に、メール情報、辞書情報及びブラウザ情報をまとめて初期設定情報と呼ぶことにする。

【0084】次いで、設定登録手段21が、WEBブラウザなどから初期設定情報を受け取り、CGIプログラム22に渡し（手順1-3）、CGIプログラム22が、WEBブラウザなどから初期設定情報を受け取り、初期設定情報から初期設定情報ファイルD11を作成する（手順1-4）。

【0085】初期設定情報ファイルD11を作成した時点で手順1が終了する。なお、パソコン環境の登録の仕方は、上記具体例に限定されるものではなく、レンタルオフィスLO1のサーバS1に、パソコン環境（パソコ

ン環境の内容も上記事項に限定されない）を自己専用パソコンCから登録できれば、その手法は問わない。

【0086】<<手順1'>>初期設定情報ファイルD11が手順1で登録された後、メイン制御手段6は、サーバS1～SNに対して、初期設定情報ファイルD11をコピーする。これにより、全てのサーバに初期設定情報ファイルD11が作成される。

【0087】<<手順2>>手順2は、初回の利用者が、利用者の正当性を認証し、上記手順1で登録した環境をパソコンSC1jに構築する手順である。なお、このとき、共通初期アプリケーション環境の復元が終了していることを条件とする。即ち、パソコンC1jのハードディスクHDが、共通初期アプリケーション環境になっていればよい。共通初期アプリケーション環境復元、及びその前提となる共通初期アプリケーション環境作成についての詳細は後述する。

【0088】先ず、利用者は、パソコンC1jに接続されたICカードR/W4にICカード3（ここで、カードIDはID=iとする）を挿入（又は提示）する（手順2-1）。

【0089】次に、利用者は、パソコンC1jの画面から、上記手順1で事前に登録した「ユーザ名、パスワード、及びカード発行時にユーザのみがICカード3にアクセス可能に設定したカードパスワード」を、図示しない表示画面を見ながら、入力手段5にて投入し、メイン制御手段6が、当該投入されたデータ群を格納する（手順2-2）。すると、メイン制御手段6は、カード情報読み書き手段7に対して、ICカード3に記憶してあるカードIDと鍵Xiの読み出しを指示すると共に、当該格納したカードパスワードをカード情報書き込み手段7に渡す（手順2-3）。

【0090】カード情報読み書き手段7が、当該指示及びカードパスワードを受け取ると、受け取ったカードパスワードをICカード3上で照合の上、カードID及び鍵Xiの読み出しを行い、メイン制御手段6にカードIDと鍵Xiを渡す（手順2-4）。すると、メイン制御手段6が、サーバS1上のカードIDがiに対応するレコードを検索して、当該レコード上のユーザ名とパスワードを読み出した後に、ユーザ名とパスワードが、入力されたデータとそれぞれ同一か判断して確認した上で、初期設定情報ファイルD11から初期設定情報を読み出す（手順2-5）。

【0091】その後、メイン制御手段6は、手順2-5で読み出した初期設定情報に対応した初期環境を構築する（手順2-6）。具体的には、例えば、メイン制御手段6は、メール情報、辞書情報、ブラウザ情報を、スクリプト作成手段8に渡して、メールスクリプト、辞書スクリプト、ブラウザスクリプト（各スクリプトはスクリプト実行手段9のインタプリタ上にて実行可能なスクリプト言語）を作成し、ハードディスクHDに渡し、ハー

ドディスクHDに格納される。そして、スクリプト実行手段9が、ハードディスクHDから各スクリプトを読み出し、各スクリプトが実行される。これにより、メールソフト、辞書、WEBブラウザの初期設定入力動作を利用者に代わってスクリプト実行手段9が行い、初期の環境構築がなされる。即ち、パソコンC1jのハードディスクHDが、スクリプト実行手段9により、共通初期アプリケーション環境から1回目初期環境になる。なお、図4におけるハードディスクHD内の各環境の包含関係は、図示した関係に限らない。以上が、手順2に関する詳細である。

【0092】<<手順4>>手順4は、パソコンC1jの利用が終了の際に、利用環境をサーバS1に保存する手順である。なお、終了時に行う必然性はなく、パソコンC1jを使用中、定期的、任意に行ってもよい。ここでのポイントは、利用者がバックアップすること自体に要する時間を極力短くすること、パソコンC1jからサーバS1へ送られかつ、サーバS1で記憶される情報が、パソコンC1j内(ICカード3内を含む)で暗号化されること、等が挙げられる。以下の説明においては、パソコン終了時における場合を取り上げる。

【0093】メイン制御手段6は、サーバS1からCDROM作成時刻情報23(詳細は後述する)を読み出すと共に、差分抽出手段11を起動させ、読み出したCDROM作成時刻情報23を差分抽出手段11に渡す(手順4-1)。

【0094】そして、差分抽出手段11は、ハードディスクHDに記録されているファイルについて、CDROM作成時刻情報23以前に作成されたファイル群を初期アプリケーション未変更ファイル群として、その他のファイル群を初期アプリケーション変更ファイル群として、それぞれ認識する一方、差分抽出手段11は、暗号化差分ファイル群D12のファイル情報(ファイル名と更新日時)と初期アプリケーション環境変更ファイル群のファイル情報(ファイル名と更新日時)とを比較し、以下の認識をする。

①暗号化差分ファイル群D12に存在せずに初期アプリケーション変更ファイル群のみに存在するファイルをコピーファイル群として認識する。

②暗号化差分ファイル群D12と初期アプリケーション変更ファイル群双方に存在するファイルについては、当該ファイルの更新日時を比較し、初期アプリケーション変更ファイル群に存在するファイルの更新日時が新しい場合のみ、コピーファイル群として認識する。

③初期アプリケーションファイル群に存在せず、暗号化差分ファイル群D12のみに存在するファイルは、削除ファイル群として認識する。

【0095】そして、上記認識に基き、差分抽出手段11は、コピーファイル群として認識したファイルについては、かかるファイル名のリストをコピーファイルリス

トとし、一方、削除ファイル群として認識したファイルについては、かかるファイル名のリストを削除ファイルリストとして、それぞれ作成する(手順4-2)。

【0096】差分抽出手段11が、コピーファイルリスト、削除ファイルリストを暗号/復号化サーバ読み書き手段12に送る(手順4-3)。

【0097】暗号/復号化サーバ読み書き手段12は、メイン制御手段6から得たコピーファイルリストに対応するファイルを順番にファイル単位で鍵Xiで各々暗号化し(ここでの暗号のアルゴリズムについては、任意の共有鍵暗号アルゴリズムでよく、暗号化の手法自体は問わない)、ファイル構造(ディレクトリやファイルの更新日時など)を保存した状態で、サーバS1上の当該ICカード3のカードID(カードID=i)の領域に暗号化差分ファイル群D12としてコピーする一方、差分抽出手段11から送られた削除ファイルリストに対応するファイルを、サーバS1上の当該ICカード3のカードID(カードID=i)の領域の暗号化差分ファイル群D12から削除する(手順4-4)。

【0098】以上、パソコンC1j使用終了後に暗号化差分バックアップの手法の一例である。ここでは、パソコンC1j使用終了時点でハードディスクHDに格納される情報とサーバS1に格納される情報が一致する様に、暗号化差分ファイル群D12が更新・削除されて一致すれば、その手法については問わない。

【0099】例えば、上記手順によれば、暗号化は全てパソコンC1jの暗号/復号化サーバ読み書き手段12で行っているが、ICカード3内にてなされても何ら問題はない。つまり、暗号/復号化サーバ読み書き手段12を暗号/復号化手段とサーバ読み書き手段とにわけ、更に、当該暗号/復号化手段を当該ICカード3に内蔵し、鍵Xiを先の手順2で読み出すことなく行うこともできる。かかる場合には、暗号化プログラム、復号化プログラムがICカード3内に格納されていることが条件となる。以上が手順4に関する詳細である。

【0100】<<手順9>>手順9は、2回目以降において、同一の利用者がレンタルオフィスLok(k≠1)を使用することを思い立った場合の手順である。本手順は、WEBブラウザCWからレンタルオフィスLO1のサーバS1上で起動中の認証手段24にアクセスする。WEBブラウザCWは、自己専用パソコンCであってよく、iモード等の携帯型WEBブラウザでもよく、また、他のインターネットにアクセスできる如何なるパソコンのWEBブラウザでもよい。具体的には、以下の通りである。

【0101】まず、WEBブラウザCWからサーバS1で起動中の認証手段24(WEBサーバなどで構成)にアクセスすると、CGIプログラム22が起動され、WEBブラウザCWには、ユーザ名とパスワードを入力要求するユーザ認証画面を表示する。利用者は、ユーザ認

証画面で「ユーザ名、パスワード」を入力する。すると CGI プログラムは、初期設定情報ファイルの利用者に対応するレコードのユーザ名とパスワードを読み出した後に、そのユーザ名とパスワードがユーザが入力したデータと同一か判断して確認した上で、WEB ブラウザ C W には、「次に利用するレンタルオフィス番号」を入力要求する画面を表示する。利用者は、次に利用する任意のレンタルオフィス番号 (1~N、ここでは k とする) を入力する。それを受けて CGI プログラム 22 は、サーバ S 1 上の暗号化差分ファイル群 D 1 2 をサーバ S k

10 にコピーする。
【0102】<<手順 6>> 手順 6 は、二回目以降において同一の利用者が、レンタルオフィス L O k を使用する手順である。まず、利用者の正当性を認証することが必須となり、手順 4 に従ってバックアップした暗号化差分ファイル群 D 1 2 をパソコン C k j (前回使用したパソコンである必要性はない) に、復元させることになる。以下に、その例を説明する。

【0103】利用者は、パソコン C k j に接続した IC カード R/W 4 にカード ID が i である自分の IC カード 3 を挿入 (又は提示) する (手順 6-1)。

【0104】次に、利用者は、パソコン C k j の画面から、上記手順 1 で事前に登録してある「ユーザ名、パスワード、及びカード発行時にユーザのみがカードにアクセス可能に設定したカードパスワード」を、図示しない表示画面を見ながら、入力手段 5 にて投入し、メイン制御手段 6 が、当該投入されたデータ郡を格納する (手順 6-2)。すると、メイン制御手段 6 は、カード情報読み書き手段 7 に対して、IC カード 3 に記憶してあるカード ID と鍵 X i の読み出しを指示すると共に、当該格納したカードパスワードをカード情報読み書き手段 7 に渡す (手順 6-3)。

【0105】カード情報読み書き手段 7 が、当該指示及びカードパスワードを受け取ると、受け取ったカードパスワードを IC カード 3 上で照合の上、メイン制御手段 6 にカード ID (ここでは、i) 及び鍵 X i を渡す (手順 6-4)。

【0106】すると、メイン制御手段 6 は、サーバ S 1 上のカード ID が i に対応するレコードを検索して、当該レコード上のユーザ名とパスワードを読み出した後に、ユーザ名とパスワードが、ユーザが入力したデータと同一か判断して確認した上で、暗号/復号化サーバ読み書き手段 12 にリストア指示を送る (手順 6-5)。

【0107】その後、暗号/復号化サーバ読み書き手段 12 は、メイン制御手段 6 からのカード ID 及び鍵 X i とを受け取り、暗号化差分ファイル群 D 1 2 のファイル群を順番に読み出し、鍵 X i で復号化しながら (復号化の手法は、手順 4 において利用した任意の共有鍵暗号手法でよい)、逐次ハードディスク HD に書き込む (手順 6-6)。つまり、ハードディスク HD が共通初期アプ

リケーション環境から 2 回目以降初期環境になる。之により、2 回目以降の初期環境が生成され、前回使用した際と同じ環境を構築できる。

【0108】ここでも、手順 4 の暗号化の際と同様に、復号化は IC カード 3 内にてなされても何ら問題はない。以上が手順 6 に関する詳細である。

【0109】<<共通初期アプリケーション環境作成>> ここで、共通初期アプリケーション環境作成につき詳細する。以下、レンタルオフィス L O 1 ~ L O N についての共通処理なので、レンタルオフィス L O 1 についてのみ説明する。この共通環境アプリケーション環境作成は、レンタルオフィスをオープンした際に、レンタルオフィス L O 1 の提供者 (オフィスサービス提供者) が 1 度だけ行う必要がある。

【0110】具体的には、以下の手法が考えられるが、別に之に限定されるものではない。例えば、全利用者の共通初期アプリケーション環境の入った起動用記録媒体 (CDROM 1 など) を、Drive Image PRO といったハードディスク HD 上の全てのデータを一括して保存時の状態に復元可能にするアプリケーション (公知) を使用して、共通初期アプリケーション環境を作成する一方、CDROM 作成直後に、その時刻情報をサーバ S 1 に CDROM 作成時刻情報 2 3 として格納する手法がある。

【0111】このとき、保存する共通初期アプリケーション環境のデータとして、初期設定設定データベースで指定できるメールソフト種別、漢字変換 I M E 種別、WEB ブラウザ種別に対応するアプリケーションがインストールされている必要がある。また、その他の文書等の作成用アプリケーション、レンタルオフィス L O 1 のパソコン C 1 j で提供されるサービスのアプリケーションもインストールされる必要がある。以上が、共通初期アプリケーション環境作成の手順である。

【0112】<<共通初期環境アプリケーション環境の復元>> また、共同利用コンピュータシステム装置 α は、共同利用パソコンを構成の一要素とするため、一人の利用者に係る情報のセキュリティを確保すると共に、何れの利用者が共同利用パソコンを使用する際に、同一の環境を整備しておく必要がある。その作業が共通初期アプリケーション環境の復元である。

【0113】利用者は、<<共通初期アプリケーション環境作成>> で作成した起動用記録媒体 (起動用 CDROM 1) をパソコン C 1 j に付属する起動用記録媒体ドライブ (CDROM ドライブ 2) に挿入し、パソコン C 1 j の電源を投入する。すると、例えば CDROM 1 からブート後に、ハードディスク HD 上に、前記初期アプリケーションである「OS、利用可能なソフト (メールソフト、WEB ブラウザ、辞書、その他のアプリケーション)」を展開することになる。なお、別にレンタルオフィス提供者が行うことも考えられる。

10

20

30

40

50

【0114】＜＜手順8＞＞なお、例えば、図1の共同利用コンピュータシステム装置αにて、会社Cの自己専用パソコンCCからの上記手順1を踏まない場合、即ち、レンタルオフィスLO1を使用したいとにわかに思い立ったとき、また、特に手順1を行うまでの当該利用者に係る利用環境に関する情報の登録の手間を惜しまない場合では、レンタルオフィスLO1に赴き、共通初期環境アプリケーション環境下で、以下の手順8を踏むことになる。

【0115】利用者は、パソコンC1jに接続したICカードR/W4にカードIDがiである自分のICカード3を挿入（又は提示）する（手順8-1）。次に、利用者は、パソコンC1jの画面から、「ユーザ名、パスワード、及びカード発行時にユーザのみがカードにアクセス可能に設定したカードパスワード」を、図示しない表示画面を見ながら、入力手段5にて投入し、メイン制御手段6が、当該投入されたデータ群を格納する（手順8-2）。

【0116】すると、メイン制御手段6は、カード情報読み書き手段7に対して、ICカード3に記憶してあるカードIDと鍵Xiの読み出しを指示すると共に、当該格納したカードパスワードをカード情報読み書き手段7に渡す（手順8-3）。以上は、上記手順6と同じ手順を行うことで達成できるものであり、実施（プログラム化等）の際の手間を省くことができる。又、ユーザ名、パスワード及びカードIDは、かかる時（又は暗号化差分バックアップ処理の最初に）、サーバS1初期設定情報ファイルD11に設定されることになる。

【0117】上述の手順の流れを整理すると、図6のようになる。複数の拠点にサーバを持つ共同利用コンピュータシステム装置の共同利用コンピュータ（シェアードピシィ）の使用で、前回利用した拠点と次に利用する拠点とが異なる場合に関する標準的な手順は、ST1→ST2→ST3→ST3'→ST4→ST5→ST10→ST11→ST12→（ST13→）ST14→ST1→ST15→ST16→ST8→ST9→ST10→ST11→ST12→（ST13→）ST14→・・・である。ここで、共同利用コンピュータ（シェアードピシィ）は、共通初期アプリケーション環境の作成が事前になされているものとする。

【0118】なお、このプロセス自体も特に、上記本発明の特徴を一側面から示したものであり、下記する効果を奏する範囲において、又システムの構成態様に応じて、適宜変更実施し得るものである。

【0119】以上、本発明の実施形態を説明したが、本発明は、必ずしも上記した事項に限定されるものではなく、本発明の目的を達し、下記する効果を奏する範囲において、適宜変更実施可能である。

【0120】

【発明の効果】本発明によれば、ある拠点のサーバ（第

1サーバ）支配下の共同利用コンピュータの利用後に、他の拠点のサーバ（第2サーバ）支配下の共同利用コンピュータを使用する場合にのみ、第1サーバに記憶された暗号化差分情報を、第2サーバに複写するので、共同利用コンピュータが複数の拠点に存在し、かつ各拠点で共同利用コンピュータが同一のサーバを利用する場合に、全拠点のサーバ間でミラーリング方法を用いる手法と比較して、通信網のトラフィック、サーバの負荷及びサーバのファイル容量を軽減することが可能となり、場所にとらわれず、異なる複数の拠点のサーバで自分のパソコン環境を即座に且つ高いセキュリティで復元することが実現できるという優れた効果を奏する。

【図面の簡単な説明】

【図1】本発明の一実施形態である共同利用コンピュータ利用方法を説明する為の共同利用コンピュータシステム装置の構成図である。

【図2】本発明の一実施形態である共同利用コンピュータ利用方法を説明する為の図1とは別の共同利用コンピュータシステム装置の構成図である。

【図3】図1における共同利用コンピュータシステム装置における、図1とは別の共同利用コンピュータ利用方法の形態を示したものである。

【図4】図1における共同利用コンピュータシステム装置における内部の構成図である。

【図5】本発明の一実施形態である共同利用コンピュータ利用方法の手順1における画面表示の一例である。

【図6】本発明の一実施形態である共同利用コンピュータ利用方法の全体の流れ図である。

【符号の説明】

α、α1…共同利用コンピュータシステム装置

C…会社

CC…自己専用パソコン

C11、C1j、CN1、CNj…共同利用パソコン（パソコン）

CW…WEBブラウザ

D11…初期設定情報ファイル

D12…暗号化差分ファイル群

G…画面

GW…ゲートウェイ

HD…ハードディスク

NW…外部通信網

NWC、NW1、NWN…内部通信網

L…ライン

LO1、LON…レンタルオフィス

1…CDROM

2…CDROMドライブ

3…ICカード

4…ICカードR/W

5…入力手段

6…メイン制御手段

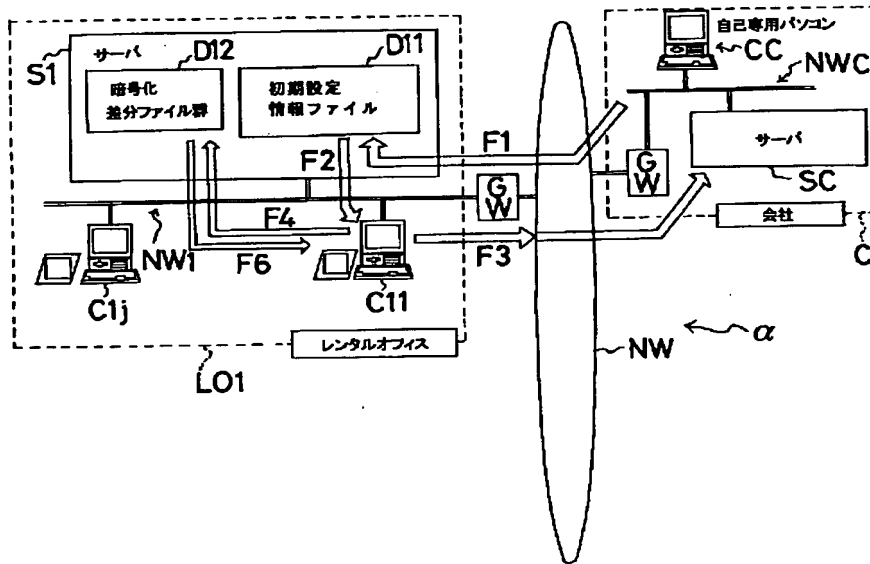
25

- 7…カード情報読み書き手段
- 8…スクリプト作成手段
- 9…スクリプト実行手段
- 10…共通初期アプリケーション復元手段
- 11…差分抽出手段
- 12…暗号／復号化サーバ読み書き手段
- 21…設定登録手段

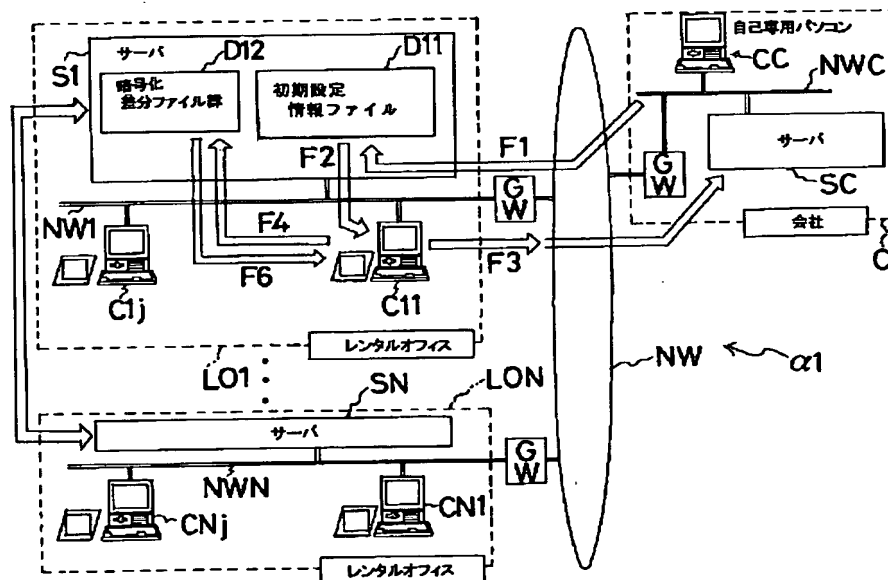
26

- 22…CGIプログラム
- 23…CDROM作成時刻情報
- 24…認証手段
- 31…辞書
- 32…ブックマーク
- 33…WEBブラウザ／FTPクライアント

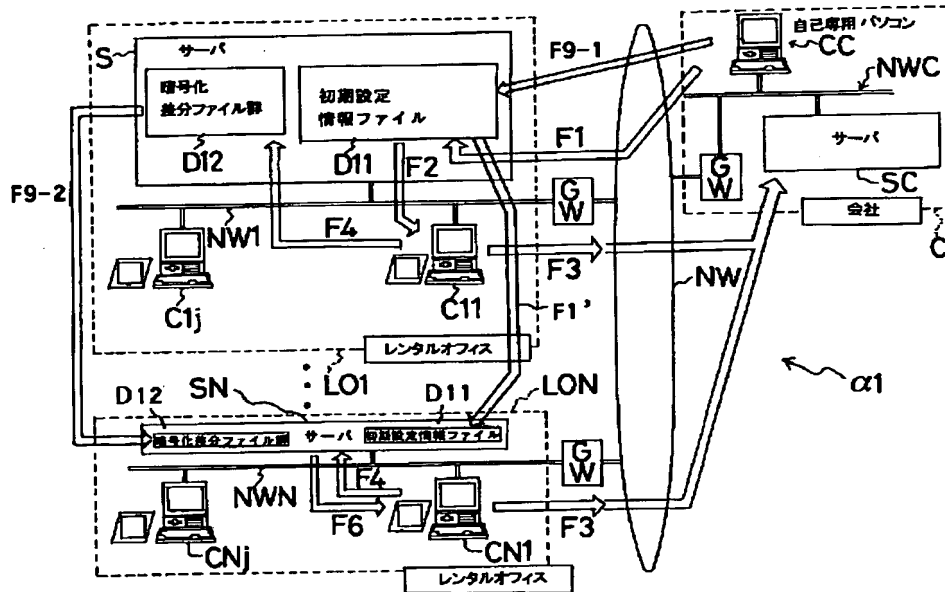
【図1】



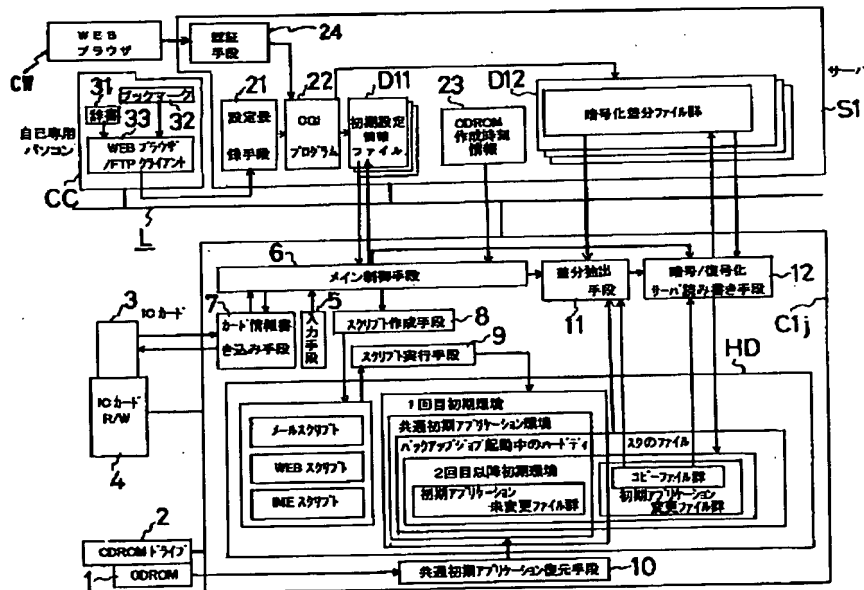
【図2】



【図3】



【図4】



【図5】

| | |
|-----------|---|
| ユーザ名 | <input type="text"/> |
| カードID | <input type="text"/> |
| パスワード | <input type="text"/> |
| メールソフト種別 | <input checked="" type="checkbox"/> メールソフト1 <input type="checkbox"/> メールソフト2 <input type="checkbox"/> メールソフト3 |
| POPサーバ名 | <input type="text"/> |
| SMTPサーバ名 | <input type="text"/> |
| メールアカウント | <input type="text"/> |
| 漢字変換IME種別 | <input checked="" type="checkbox"/> IME1 <input type="checkbox"/> IME2 |
| WEBブラウザ種別 | <input checked="" type="checkbox"/> ブラウザ1 <input type="checkbox"/> ブラウザ2 |

← G

【図6】

